EXHIBIT 13

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al.*,	:	
	:	
Plaintiffs,	:	
	:	
v.	:	**CIVIL ACTION NO. 1:17-CV-2989-AT**
BRIAN KEMP, *et al.*,	:	
	:	
Defendants.	:	

ORDER

contracted with Kennesaw State University to maintain the central server for the State at a unit in the University called the Center for Election Services ("CES"). Plaintiffs allege that the central server was accessible via the internet for a time – at least between August 2016 and March 2017.

In August 2016, Logan Lamb, a professional cybersecurity expert in Georgia, went to CES's public website and discovered that he was able to access key election system files, including multiple gigabytes of data and thousands of files with private elector information. The information included electors' driver's license numbers, birth dates, full home addresses, the last four digits of their Social Security numbers, and more. Mr. Lamb was also able to access, for at least 15 counties, the election management databases from the GEMS central tabulator used to create ballot definitions, program memory cards, and tally and store and report all votes. He also was able to access passwords for polling place supervisors to operate the DREs and make administrative corrections to the DREs. Immediately, Mr. Lamb alerted Merle King, the Executive Director overseeing CES, of the system's vulnerabilities. The State did not take any remedial action after Mr. King was alerted.

In February 2017, a cybersecurity colleague of Mr. Lamb's, Chris Grayson, was able to repeat what Mr. Lamb had done earlier and access key election information. Mr. Lamb also found, around this time, that he could still access and download the information as he had before. On March 1, 2017, Mr. Grayson notified a colleague at Kennesaw State University about the system's

vulnerabilities, and this led to notification of Mr. King again. Days later, the FBI was alerted and took possession of the CES server.

The Secretary of State has since shut down the CES and moved the central server internally within the Secretary's office. But on July 7, 2017, four days after this lawsuit was originally filed in Fulton Superior Court, all data on the hard drives of the University's "elections.kennesaw.edu" server was destroyed. And on August 9, 2017, less than a day after this action was removed to this Court, all data on the hard drives of a secondary server – which contained similar information to the "elections.kennesaw.edu" server – was also destroyed. As discussed more fully later in this Order, the State offered little more than a one-sentence response to these data system incursions and vulnerabilities at CES.

The Premier/Diebold voting machine models at issue have been the subject of comprehensive critical review both by university computer engineer security experts independently as well as under the auspices of the States of Maryland, California, and Ohio. These studies identified serious security vulnerabilities in the software and resulted in the three states' adoption of different voting systems. (Halderman Affidavit, Doc. 260-2 ¶¶ 17-23; *see also* Atkeson Affidavit, Doc. 276-1 ¶¶ 8-9 (also discussing the states of New Mexico and Virginia transitioning away from DREs after identifying several issues with the machines).)[8]

[8] By contrast, the Secretary of State certified in April 2018 the accuracy and safety of the Georgia DRE system. This certification was based on a pre-announced examination of voting facilities and the conducting of a tiny mock election in several Georgia counties on November 27-29, 2017 by a combination of staff from the Secretary of State's Office and the Center for Election Services at Kennesaw State University. (Def. Ex. 2 from Preliminary Injunction Hearing.) No

> that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of. . . . Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

United States v. Hays, 515 U.S. 737, 742–43 (1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–561 (1992)) (internal quotation marks omitted). "[A] plaintiff must demonstrate standing for each claim he seeks to press and for each form of relief that is sought." *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650 (2017) (quoting *Davis v. Federal Election Comm'n*, 554 U.S. 724, 734 (2008)).

As to the first element, Defendants contend that Plaintiffs have not sufficiently alleged a concrete "injury in fact." Defendants argue that Plaintiffs' allegations that the DRE voting machines are vulnerable to hacking and are "presumed to be compromised" convey only a speculative, generalized fear, thus falling short of establishing a concrete injury.

These arguments are unavailing. For one, Plaintiffs have alleged that the DRE voting system was *actually* accessed or hacked multiple times already – albeit by cybersecurity experts who reported the system's vulnerabilities to state authorities, as opposed to someone with nefarious purposes. (Curling Complaint, Doc. 70 ¶¶ 42-43, 45-49; Coalition Complaint, Doc. 226 ¶¶ 95-106.) Contrary to Defendants' characterizations, Plaintiffs' allegations are not premised on a

theoretical notion or "unfounded fear"[19] of the hypothetical "possibility" that Georgia's voting system might be hacked or improperly accessed and used. Plaintiffs allege that harm has in fact occurred, specifically to their fundamental right to participate in an election process that accurately and reliably records their votes and protects the privacy of their votes and personal information. (Curling Complaint, Doc. 70 ¶ 14 ("Curling also chose to exercise her right to cast her vote using a verifiable paper ballot in the Runoff, so as to ensure that her vote would be permanently recorded on an independent record. To do so, Curling persisted through considerable inconvenience – only to be incorrectly told by Defendants Kemp and the Fulton County Board of Registration and Elections that she had not, in fact, cast a ballot, creating irreparable harm that her ballot was not counted."); ¶ 16 (Donna Price "cast her vote on a DRE in the 2016 General Election," and "[w]ithout the intervention of this Court, Price will be compelled to choose between relinquishing her right to vote and acquiescing to cast her vote under a system that violates her right to vote in absolute secrecy and have her vote accurately counted"); ¶ 38 ("DREs produce neither a paper trail nor any other means by which the records of votes cast can be audited."); ¶¶ 42-43 ("Lamb was able to access key components of Georgia's electronic election infrastructure . . . . In accessing these election system files, Lamb found a startling amount of private information," including driver's license numbers, birth dates, and the last four digits of Social

[19] *See* State Defendants' Motion to Dismiss Coalition Plaintiffs' Third Amended Complaint, Doc. 234-1 at 1.

Security numbers); Coalition Complaint, Doc. 226 ¶ 152 (member of CGG, Brian Blosser, "was prohibited from voting on April 18, 2017 . . . when his name did not appear on the eligible voter rolls" for the Sixth Congressional District and "was instead erroneously listed" as a resident of another district, an error that Fulton County Board members blamed on a "software glitch"); ¶ 154 (members of CGG, Mr. and Ms. Digges, previously in 2017 "chose to vote by mail-in paper absentee ballot because they were aware that an electronic ballot cast using an AccuVote DRE was insecure," and they "were required to undergo the inconvenience of requesting paper ballot[s] and the cost of postage to mail their ballots" "well before Election Day"); ¶ 72 ("Georgia's AccuVote DREs do not record a paper or other independent verifiable record of the voter's selections."); ¶ 92 ("[D]esign flaws render the electronic ballots cast on AccuVote DREs capable of being matched to voter records maintained by pollworkers and pollwatchers," and thereby expose citizens' candidate selections to poll workers); ¶ 97 ("Lamb freely accessed files hosted on the 'elections.kennesaw.edu' server, including the voter histories and personal information of all Georgia voters . . . . Lamb noted that the files had been publicly exposed for so long that Google had cached (i.e., saved digital backup copies of) and published the pages containing many of them."); ¶ 138 ("Fulton Board Members have adopted voting procedures under which individual electronic ballots bearing a unique identifier are transmitted from Fulton County's AccuVote DREs located in satellite voting centers to Fulton County's central GEMS tabulation server in clear text (i.e., unencrypted) over an ordinary, unsecured

telephone line on Election Night. This practice violates fundamental security principles because it subjects the transmitted votes to manipulation (such as man-in-the-middle interception and substitution of votes) and exposes the votes with their unique identifier to third-party interception, violating voters' rights of secrecy in voting.").)

Plaintiffs also allege the threat of future harm. For instance, in upcoming elections, Plaintiffs allege that Defendants are requiring them to vote early, mail a paper absentee ballot, and pay for postage to avoid having to use unsecure DRE machines, thereby subjecting them to unequal treatment. Furthermore, Plaintiffs plausibly allege a threat of a future hacking event that would jeopardize their votes and the voting system at large. Despite being aware of election system and data cybersecurity threats and vulnerabilities identified by national authorities and the DRE system's vulnerability to hacking as early as August 2016 – when Logan Lamb, the computer scientist, first alerted the State's Executive Director of the CES of his ability to access the system – Defendants allegedly have not taken steps to secure the DRE system from such attacks. (Curling Complaint, Doc. 70 ¶ 46 ("[N]ot only did Georgia fail to take remedial action when alerted to the problem Lamb raised, it failed to act even in the face of the detailed information on the cybersecurity threats facing the nation's election systems, and the recommended specific steps to reduce the risk, which were disseminated by the FBI, the DHS and

the EAC[20].”); Coalition Complaint, Doc. 226 ¶ 112 (“[N]o efforts have been made to remediate the compromised software programs and machines or to identify and remove any malware that was likely introduced during the lengthy security breaches referred to herein on the ‘elections.kennesaw.edu’ server that hosted the election-specific software applications and data that are re-installed on every piece of voting and tabulation equipment used to conduct Georgia’s elections in advance of each election conducted using Georgia’s Voting System.”).)

Importantly, courts have recognized these sorts of alleged harms as concrete injuries, sufficient to confer standing. In particular, courts have found that plaintiffs have standing to bring Due Process and Equal Protection claims where they alleged that their votes would likely be improperly counted based on the use of certain voting technology. *See, e.g.*, *Stewart v. Blackwell*, 444 F.3d 843, 855 (6th Cir. 2006) (“The increased probability that their votes will be improperly counted based on punch-card and central-count optical scan technology is neither speculative nor remote.”), *vacated* (July 21, 2006), *superseded*, 473 F.3d 692 (6th Cir. 2007) (vacated and superseded on the grounds that the case was rendered moot by the county’s subsequent abandonment of the DRE machines at issue); *Banfield v. Cortes*, 922 A.2d 36, 44 (Pa. Commw. Ct. 2007) (finding that the plaintiffs had sufficiently alleged standing under similar Pennsylvania law, based on “the fact that Electors have no way of knowing whether the votes they cast on a

[20] DHS is the acronym for the U.S. Department of Homeland Security, and EAC is the acronym for the U.S. Election Assistance Commission.

DRE have been recorded and will be counted," which "gives Electors a direct and immediate interest in the outcome of this litigation"); *c.f. Stein v. Cortes*, 223 F. Supp. 3d 423, 432-33 (E.D. Pa. 2016) (where plaintiffs sought a vote recount, post-election, based on the use of unsecure DREs, finding no standing based on the plaintiffs' "less than clear" allegations that the DRE machines are "hackable"; that the Pennsylvania Election Code's recount provisions are "labyrinthine, incomprehensible, and impossibly burdensome"; and that the past vote count was inaccurate – which plaintiffs merely posed as a "seemingly rhetorical question").

Turning to causal connection, the second element of standing, Defendants raise different arguments in response to the Curling Plaintiffs' claims versus the Coalition Plaintiffs' claims. For the Curling Plaintiffs, Defendants argue that any injury would be traced to illegal hacking into the DREs, not the use of the DREs themselves. Here, as discussed above, the Curling Plaintiffs have alleged that Defendants were aware of serious security breaches in the DRE voting system and failed to take adequate steps to address those breaches. Notably, even after Mr. Lamb first alerted the State about his access of the voting system, he and another cybersecurity expert were able to access the system *again* about six months later. (Curling Complaint, Doc. 70 ¶ 47.) Plaintiffs allege that Defendants have continued to fail to take action to remedy the DRE system's vulnerabilities. (*Id.* ¶¶ 46, 61, 62, 72.) And they allege that this failure, in turn, impacts the integrity of the voting system and their ability as citizens to rely upon it when casting votes in this system. (*Id.*) At the motion to dismiss stage, these allegations plausibly show

causal connection, even if indirectly, between Defendants' continued use of unsecure DREs and the injury to Plaintiffs' constitutional rights. *Focus on the Family v. Pinellas Suncoast Transit Auth.*, 344 F.3d 1263, 1273 (11th Cir. 2003) ("[E]ven harms that flow indirectly from the action in question can be said to be 'fairly traceable' to that action . . . .").

For the Coalition Plaintiffs, Defendants make the same argument above regarding causation (which fails) and another slightly different argument. Defendants take issue with the Coalition Plaintiffs' request for relief enjoining the State Defendants from enforcing O.C.G.A. § 21-2-383(b) and State Election Board Rule 183–1–12–.01. Defendants assert that the State Defendants (the Secretary and the State Election Board) do not mandate the use of DREs; rather, state law requires the use of DREs. Defendants maintain that the State Defendants are merely implementing the governing state law, which they are bound to do, and therefore Plaintiffs miss the mark by seeking to enjoin the State Defendants' actions instead of challenging the state law itself. In this way, Defendants argue that Plaintiffs have not linked their injury to any action by the State Defendants.

But O.C.G.A. § 21-2-383(b) does not *require* the use of DREs as Defendants claim it does. The statute requires absentee electors who vote in-person in the advance voting period to vote by DRE, but only "in jurisdictions in which direct recording electronic (DRE) voting systems are used at the polling places on election day." The statute simply specifies the use of DREs under certain circumstances. Rather, it is the State Election Board that issued a rule requiring

the use of DREs in "all federal, state, and county general primaries and elections, special primaries and elections, and referendums," and requiring the use of DREs by "persons desiring to vote by absentee ballot in person." Ga. Comp. R. & Regs. r. 183–1–12–.01. When read together, the state statute and the State Election Board rule indicate that the State Defendants have chosen to enforce state law so as to generally require the use of DREs in elections statewide.

Even apart from the statutory language, the Coalition Plaintiffs have plausibly alleged that the State Defendants play a critical role in directing, implementing, programming, and supporting the DRE system throughout the state. The Coalition Plaintiffs allege that the Secretary provided the counties with the DRE machines and the software on which they operate. (Coalition Complaint, Doc. 226 ¶ 59.) Additionally, from 2002 to December 2017, the Secretary allegedly contracted with Kennesaw State University to create the Center for Election Services ("CES") "to assist the Secretary in the fulfillment of his statutory duties to manage Georgia's election system." (*Id.* ¶ 93.) The CES maintained a central computer server containing sensitive voting-related information such as software applications, voter registration information, ballot building files, and "other sensitive information critical to the safe and secure operation of Georgia's Voting System." (*Id.* ¶¶ 94, 119.) These factual allegations, when considered with the Third Amended Complaint as a whole, show that the Coalition Plaintiffs have alleged enough of a causal link between the State Defendants' conduct and their injury for standing purposes.

Finally, on the third element of redressability, Defendants raise some of the same arguments as they do for the second element. Defendants argue that an injunction prohibiting the State Defendants from using DREs would not actually stop the deployment of DREs. Defendants maintain that county officials not included in this suit would continue to use DREs, as the State is not the entity that enforces the law requiring DREs. Defendants also argue that a different balloting system would not eliminate potential third-party interference, as no election system is flawless.

As stated above, the Court finds that the Coalition Plaintiffs have sufficiently alleged that the State Defendants play a significant role in the continued use and security of DREs, and therefore the requested injunction would help redress some of the Coalition Plaintiffs' injury. The Secretary of State both has the authority and obligation to investigate complaints regarding the accuracy and safety of the DRE voting system and to take appropriate corrective action in connection with the continued use of the DRE system. O.C.G.A. § 21-2-379.2. The Third Amended Complaint describes how the Secretary of State could play a critical role in conducting an in-depth investigation and formulating a remedy. As alleged in the Complaint, the State of California commissioned a study in 2007 to examine the security of its own Diebold AccuVote DRE system, the same type of system used in Georgia. Upon the study's findings that the DRE system was inadequate, had serious design flaws, and was susceptible to hacking, California's Secretary of State then decertified its DRE system in 2009. (Coalition Complaint, Doc. 226 ¶¶ 81,

84, 86.) The Complaint similarly alleges that the Secretary of State for Ohio commissioned an independent expert study of a newer version of the DREs than those used in Georgia and reached similar conclusions as to the lack of trustworthy design and vulnerability to attack of the election system. (*Id.* ¶¶ 81, 83, 85.)

The State Defendants here are similarly in a position to redress the Plaintiffs' alleged injury. Thus, if the Court were to grant at least part of the requested injunctive relief as to the suspended use of the DRE voting system, any injunction would likely enjoin both the State Defendants as well as the Fulton County Defendants (as there is no argument that the County would not be enjoined). Furthermore, as to Defendants' argument that no election system is flawless, the Coalition Plaintiffs rightly point out that this is not the standard for redressability. Plaintiffs are seeking relief to address a particular voting system which, as currently implemented, is allegedly recognized on a national level to be unsecure and susceptible to manipulation by advanced persistent threats through nation state or non-state actors. Plaintiffs are not asking for a system impervious to all flaws or glitches.

Defendants assert three additional arguments related to standing: that the Coalition Plaintiffs cannot manufacture standing by inflicting harm on themselves, that the individual Plaintiff Coalition for Good Governance ("CGG") lacks organizational and associational standing, and that Plaintiffs must reside in the jurisdiction for which they seek to enjoin DRE use.

The first of these arguments fails because the cases relied on by Defendants are distinguishable. Here, the Coalition Plaintiffs are suffering injury from the voluntary exercise of their *fundamental right to vote*, not from just any sort of activity that they decide to engage in. In *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the plaintiffs voluntarily spent money to take certain protective measures, based on a hypothetical fear of being subject to surveillance. And in *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992), the plaintiffs expressed an intent to voluntarily return to certain places they had visited before, which would deprive them of the opportunity to observe animals of an endangered species. These activities do not invoke the protection associated with exercising fundamental rights, such as the right to vote. The Coalition Plaintiffs aptly point out that Defendants' logic would bar many voting rights cases, based on individuals choosing to vote by one method or another, which certainly is not how courts have assessed standing in this context.

Defendants' challenge of CGG's standing similarly fails. "An organization has standing to enforce the rights of its members when its members would otherwise have standing to sue in their own right, the interests at stake are germane to the organization's purpose, and neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Fla. State Conference of N.A.A.C.P. v. Browning*, 522 F.3d 1153, 1160 (11th Cir. 2008) (internal quotation marks omitted). The State Defendants argue that the Coalition Plaintiffs merely "presume" harm to their own members, without sufficiently

Stewart v. Blackwell, 444 F.3d at 868-72, where strict scrutiny was applied based on the plaintiffs' allegations of "vote dilution due to disparate use of certain voting technologies." 444 F.3d at 871. Thus, in contrast with *Stewart*, the Eleventh Circuit in *Wexler* did not apply strict scrutiny and instead reviewed "Florida's manual recount procedures to determine if they are justified by the State's 'important regulatory interests.'" *Wexler*, 452 F.3d at 1233 (citing *Burdick*, 504 U.S. at 434)).

Here, Plaintiffs appear to present facts that fall somewhere between *Wexler* and *Stewart*. Unlike *Wexler*, Plaintiffs are alleging that they are less likely to be able to cast accurate or effective ballots when voting by DRE. The evidence here is not as well developed as that in *Stewart*, which was decided on a fully factually developed summary judgment record. Still, Plaintiffs in this case have presented sufficient evidence so far that their votes cast by DRE may be altered, diluted, or effectively not counted on the same terms as someone using another voting method – or that there is a serious risk of this under the circumstances.

Turning to the second element for a preliminary injunction, the Court also finds that Plaintiffs have demonstrated a real risk of suffering irreparable injury without court intervention. This analysis to some extent parallels the "injury in fact" standing analysis above. Absent an injunction, there is a threat that Plaintiffs' votes in the upcoming elections will not be accurately counted. Given the absence of an independent paper audit trail of the vote, the scope of this threat is difficult

ballot requirement by limiting early voting to one central location, rather than offering it at 20 locations spread throughout the county. This, of course, would likely directly impact voter turnout and access to voting.

Ultimately, any chaos or problems that arise in connection with a sudden rollout of a paper ballot system with accompanying scanning equipment may swamp the polls with work and voters – and result in voter frustration and disaffection from the voting process. There is nothing like bureaucratic confusion and long lines to sour a citizen. And that description does not even touch on whether voters themselves, many of whom may never have cast a paper ballot before, will have been provided reasonable materials to prepare them for properly executing the paper ballots.

The Court attempted to expedite this case at earlier times to no avail. The Court understands some of the reasons why Plaintiffs may have been unable to file a preliminary injunction motion before new counsel for the Coalition Plaintiffs filed a Third Amended Complaint in June 2018. But the *August* filing of their motion for preliminary injunction effectively put the squeeze on their proposed remedial relief. Requiring injunctive relief on this broad of a scale, and on an abrupt, time-limited basis, would likely undermine a paper ballot initiative with a scanned audit trail that appears in reality to be critically needed.

Meanwhile, the State Defendants have also stood by for far too long, given the mounting tide of evidence of the inadequacy and security risks of Georgia's DRE voting system and software. The Court is gravely concerned about the State's

pace in responding to the serious vulnerabilities of its voting system – which were raised as early as 2016 – while aging software arrangements, hardware, and other deficiencies were evident still earlier. The Secretary of State's Secure, Accessible, & Fair Elections (SAFE) Commission has held just two meetings since its establishment in April 2018, though it is tasked with making recommendations to the legislature that convenes in January 2019. The State and the County's arguments about the time and resource constraints at issue, in the event the Court granted the requested injunctive relief, are compelling right now, with the November election just weeks away. But these arguments only weaken the more that time passes and if Defendants continue to move in slow motion or take ineffective or no action. For upcoming elections after November 2018, Defendants are forewarned that these same arguments would hold much less sway in the future – as any timing issues then would appear to be exclusively of Defendants' own making at that point.

Upon considering the totality of the evidence in connection with the four factors that must guide the Court's determination regarding the grant of extraordinary relief as to Plaintiffs' constitutional claims, the Court finds that the Plaintiffs have not carried their burden of persuasion to establish these prerequisites for such extraordinary injunctive relief in the immediate 2018 election time frame ahead.

V. Conclusion

While Plaintiffs' motions for preliminary injunction [Docs. 258, 260, 271] are **DENIED**, the Court advises the Defendants that further delay is not tolerable in their confronting and tackling the challenges before the State's election balloting system. The State's posture in this litigation – and some of the testimony and evidence presented – indicated that the Defendants and State election officials had buried their heads in the sand. This is particularly so in their dealing with the ramifications of the major data breach and vulnerability at the Center for Election Services, which contracted with the Secretary of State's Office, as well as the erasure of the Center's server database and a host of serious security vulnerabilities permitted by their outdated software and system operations.

A wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting.

Advanced persistent threats in this data-driven world and ordinary hacking are unfortunately here to stay. Defendants will fail to address that reality if they demean as paranoia the research-based findings of national cybersecurity engineers and experts in the field of elections. Nor will surface-level audit procedures address this reality when viruses and malware alter data results and evade or suppress detection. The parties have strongly intimated that this case is headed for immediate appeal. But if the case stays with or comes back to this Court, the Court will insist on further proceedings moving on an expedited

schedule. The 2020 elections are around the corner. If a new balloting system is to be launched in Georgia in an effective manner, it should address democracy's critical need for transparent, fair, accurate, and verifiable election processes that guarantee each citizen's fundamental right to cast an accountable vote.

IT IS SO ORDERED this 17th day of September, 2018.

Amy Totenberg
United States District Judge